CYBERSECURITY AND DATA PRIVACY
& EMPLOYEE BENEFITS LAW
INFORMATION MEMO
OCTOBER 7, 2022

Cybersecurity Awareness Month – Cybersecurity Guidance for Retirement Plans

In 2021, the US Department of Labor (DOL) issued cybersecurity best practices for retirement plan sponsors, fiduciaries, record-keepers, participants and beneficiaries, focusing on three topics: hiring service providers; managing cybersecurity risks; and online security tips for participants. Although couched as "best practices," the DOL has referred to this guidance during investigations, questioning retirement plans about how they were complying with these cybersecurity standards. As a result, the DOL may view this guidance as establishing minimum standards for retirement plans and potentially assess liability for damages stemming from plan data breaches in the future. Although the guidance did not address health and welfare plans, those plans may also wish to consider implementing some or all of these measures to guard against cyber attacks.

Below are key points raised in the above-referenced guidance, as well as some helpful insights to be considered in connection with the DOL's recommendations. For a more detailed discussion on the DOL's best practices, click here.

I. Hiring Service Providers

Under ERISA, plan fiduciaries must act prudently when selecting and retaining plan service providers. As a consequence of providing services to their plan clients, these vendors often have access to and are required to maintain and secure plan records and data. To ensure that service providers implement strong measures to defend this information against potential cyber threats, the DOL recommends that plan sponsors require their vendors implement and maintain satisfactory security systems to guard against attacks and prevent potential breaches. Importantly, this guidance is consistent with industry best practices when it comes to third-party risk and vendor management. The DOL offered a number of suggested practices when contracting with service providers, including:

- Evaluate security standards, practices, and policies and review independent audit results of these security system to verify their sufficiency and compare to industry standards.
- Review details regarding prior incidents and the response to those attacks.
- Ensure vendors maintain cybersecurity insurance policies to address losses incurred from security breaches or identity thefts and confirm policy limitations and scope of coverage.
- Implement standards to preserve the privacy of all confidential data and prevent any improper or unnecessary use or disclosure of confidential information without consent.

II. Cybersecurity Best Practices

The DOL also provided a list of best practices for plans, their record keepers and other service providers to follow, including maintaining a formal, well documented cybersecurity program, conducting prudent annual risk assessments, performing reliable third-party audits of security controls, devising strong access control procedures, conducting periodic cybersecurity awareness training and encryption sensitive data. The DOL's guidance tracks several data privacy and cybersecurity laws enacted throughout the U.S., including in New York State. For example, the New York SHIELD Act's

Cybersecurity mandate, effective in March 2020, requires all organizations holding New York resident electronic data to implement the same administrative, technical and physical safeguards couched as "best practices" in the DOL's guidance. Certainly, New York employers that maintain New York resident data are already obligated by law to comply with SHIELD Act and therefore already familiar (and in compliance) with the standards set forth as "Best Practices" by the DOL. See below for more information on compliance with NY SHIELD Act.[1]

III. Online Security Tips

The DOL also outlined a number of security tips, reflecting that participants and beneficiaries also play a large role in the security of their plan accounts. The DOL recommends that users utilize strong and unique passwords for their accounts, add multi-factor authentication to log in, and regularly monitor accounts to guard against the risk of fraud and loss. In addition, the DOL suggests that participants and beneficiaries update their contact information with plans and sign up for account activity notifications to ensure they are notified of any unauthorized account activity. Among the other tips offered, the DOL urges users to avoid public wi-fi networks, remain mindful of phishing attacks and use up-to-date antivirus software.

* * * * *

Retirement plans are literal treasure troves for cyber criminals – holding large amounts of funds and personal information concerning participants and beneficiaries. Recognizing this concern, the DOL's new cybersecurity guidance may provide a glimpse into future enforcement actions and a checklist to assess prudence by fiduciaries in the event of a cyberattack. Plans should consider these tips and insights when engaging new service providers to ensure vendors are taking appropriate precautions to safeguard plan data. They may also wish to revisit current contracts with their present vendors to address any areas where their contracts are silent, as well as consider whether additional measures are necessary to ensure the security and confidentiality of plan data.

Administrators may also wish to review and update their plans' document and retention policies to reflect this new guidance, and review their vendors' policies to confirm if amendments are warranted – with a particular focus on how vendors handle plan data upon expiration or termination of their agreement.

If you have any questions, please contact Lawrence J. Finnell, any attorney in our employee benefits and executive compensation practice, Jessica L. Copeland, any attorney in our cybersecurity and data privacy practice or the attorney at the firm with whom you are regularly in contact.

1 *See* NY SHIELD Act - Are You Ready To Comply?; NY SHIELD Act – Are Your Policies in Place?; New York SHIELD Act Now Requires Your Compliance

BOND SCHOENECK & KING ATTORNEYS